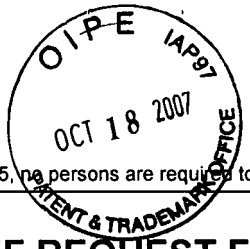
Doc Code: AP.PRE.REQ



PTo/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
JRL-550-483	

Application Number	Filed
10/713,303	November 17, 2003
First Named Inventor	
SYMES	
Art Unit	Examiner
2131	Chai, Longbit

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ Applicant/Inventor

☐ Assignee of record of the entire interest. See 37 C.F.R. § 3.71. Statement under 37 C.F.R. § 3.73(b) is enclosed. (Form PTO/SB/96)

☒ Attorney or agent of record 33,149 (Reg. No.)

☐ Attorney or agent acting under 37CFR 1.34.
Registration number if acting under 37 C.F.R. § 1,34 _____

Signature

John R. Lastova
Typed or printed name

703-816-4025
Requester's telephone number

October 18, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.*

☒ *Total of 1 form/s are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

SYMES

Atty. Ref.: 550-483; Confirmation No. 1418

Appl. No. 10/713,303

TC/A.U. 2131

Filed: November 17, 2003

Examiner: Chai, Longbit

For: APPARATUS AND METHOD FOR MANAGING PROCESSOR CONFIGURATION DATA

* * * * * * * * * * *

October 18, 2007

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

STATEMENT OF ARGUMENTS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

All claims stand rejected under 35 U.S.C. §103 for obviousness based on Candelore and Shipman. This rejection is traversed for the reasons explained in the prior response and below.

The claims are concerned with a data processing apparatus that supports both secure and non-secure operation. In secure operation, secure data should not be accessed by a non-secure part of the data processing apparatus. But a security vulnerability may arise when the processor switches between secure operation (the processor is configured to operate in a secure domain) and non-secure operation (the processor is configured to operate in a non-secure domain). The processor's configuration is determined by processor configuration data held in a storage unit accessible by the processor. When switching from the secure domain to the non-secure domain, the secure processor configuration data must be replaced in the storage unit with the non-secure processor configuration data. Similarly, if the processor is switching from the non-secure domain to the secure domain, this switching requires replacing non-secure processor configuration data in the storage unit with the secure processor configuration data.

This switching is managed by having the processor operate in a monitor mode to execute a monitor program to oversee the switching. Typically, when processor configuration data is changed in the storage unit, it is immediately effective, which may compromise the ability of the

monitor program to correctly switch of all of the required processor configuration data. To overcome this problem, the monitor program uses monitor mode specific processor configuration data when the processor operates in the monitor mode, which ensures that the processor is not affected by the switching of the processor configuration data required to implement the transition from one domain to the other.

CANDELORE LACKS THE CLAIMED MODES AND DOMAINS

Candelore lacks "a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain [and] at least one secure mode being a mode in the secure domain." The text in Candelore relied on by the Examiner refers to secure/non-secure modes and secure/non-secure system portions. In Candelore, there is *no difference* between a "mode" and a "system portion." But in the pending claims, a "mode" is *different* from a "domain." A person of ordinary skill in this art would understand in light of the specification that the claimed secure and non-secure domains provide a mechanism for handling security at the hardware level. They effectively establish separate worlds: the non-secure world groups all hardware and software accessible to non-secure applications that do not require security, and the secure world groups all hardware and software that is only accessible when executing secure code. That skilled person would also understand that in contrast, a mode of operation is only available to certain types of devices such as processors. Figures 3 and 4 below help illustrate the difference between modes and domains.

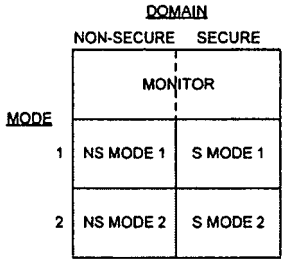


FIG. 3

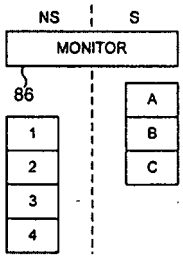


FIG. 4

In the final rejection, the Examiner disregards the fact that the two different claim terms "mode" and "domain" mean different things. In contrast, a person skilled in the art of data processing apparatus security would understand the difference between these two terms, particularly in light of the specification, and would certainly not consider them to be the same as

the Examiner does. The Examiner's unreasonable interpretation highlights the fact that Candalore fails to disclose the claimed modes and domains which are different and distinct.

CANDELORE'S A/B TIME SWITCHER IS NOT THE CLAIMED STORAGE UNIT

For the claimed "a storage unit configured to store processor configuration data," the Examiner also contends that "a mode selection signal is used by the mode A/B timer switcher" in Candelore, referring to the selection signal carried by path 380 in Figure 3 (see page 11, lines 16 to 18). But this signal simply indicates which mode the processor is currently in, and can not reasonably be considered to be "a storage unit configured to store processor configuration data."

CANDALORE LACKS THE CLAIMED MONITOR MODE

Claim 1 further recites that the plurality of modes includes "a monitor mode." The Examiner points to a switch device described in the context of Candelore's Figure 4 that issues a mode A/B selection signal (via path 380 in Figure 3). Switching occurs based on time and various time switching patterns as described on page 14. Thus, Candelore describes a system component (a switch) rather that a "mode" in which the processor is configured.

CANDELORE LACKS THE CLAIMED CONFIGURATION SWITCHING

The Examiner's position is that any data encountered or handled by the processor is "processor configuration data" because that data dictates how the processor behaves. The Examiner's interpretation of the claimed "processor configuration data" is unreasonable. The plain and ordinary meaning of the words "processor configuration data" is data used to configure the processor, i.e., how the processor is arranged or set up. A person skilled in the art of data processing apparatus security would know that "processor configuration data," understood in light of the specification, refers to configurable parameters that determine how the processor will operate on input data and instructions it receives. Processor configuration data is different from data merely provided to a processor as an input parameter during execution of a particular process, such as a password. Although an input parameter data may influence how the process executes, it has no direct bearing on the configuration of the processor. Indeed, when the processor receives that input, it is already configured.

For "switching the processor configuration data in the storage unit...," the Examiner refers to the MSB function described on page 16, lines 6 to 11 of Candelore. The MSB of the

memory address is simply a label to conveniently divide the memory into two halves. It does not alter "processor configuration data" stored in a storage unit.

Nor does the Examiner's reading of "processor configuration data" onto the MSB-bit of an address register make sense in the claim context of data processing apparatus security. For example, if a secure/non-secure configuration of a processor were defined by the MSB-bit of the address register, then merely by loading an address into the address register, the security mode of the processor could be changed. This certainly would not be secure. Even if the MSB-bit could be defined as non-alterable when the processor is in a non-secure mode, (a point not made by the Examiner), then some MSB alteration parameter within the processor would have to be checked to determine whether the MSB-bit can be altered or not. That MSB alteration parameter corresponds to "processor configuration data," but the MSB-bit itself is not processor configuration data. Accordingly, Candelore lacks "switching the processor configuration data in the storage unit between secure processor configuration data and non-secure processor configuration data," as recited in claim 1.

SHIPMAN'S SMI HANDLER DOES NOT MANAGE PROCESSOR CONFIGURATION DATA SWITCHING TO ENSURE THE PROCESSOR'S SECURITY IS UNAFFECTED

The Examiner admits that Candelore lacks the monitor mode managing feature and relies on Figure 4 in Shipman. Figure 4 illustrates keyboard controller states—not operating modes of the processor. Column 2, lines 10 to 28 and the abstract explain that Shipman's teachings specifically relate to the "security" of a keyboard controlling facility when this security is directed by a system management interrupt (SMI) handler. As in Candelore, Shipman also fails to distinguish between a "domain" and a "mode" as those terms would be understood by a person skilled in the art of data processing apparatus security in light of the specification.

The Examiner asserts that a password used by Shipman's SMI handler for a keyboard controller in a sleuth mode constitutes "monitor mode specific processor configuration data." Shipman's password is merely an input parameter provided for determining whether a transition from non-secure to secure mode is allowed. It has no meaning outside of the mode switch operation. Hence, the sleuth mode password is not the claimed "processor configuration data." In addition, equating a password to processor configuration data means that Shipman would have to disclose three different passwords: one for each of the claimed secure, non-secure, monitor mode specific processor configuration data. Shipman fails to teach these three passwords.

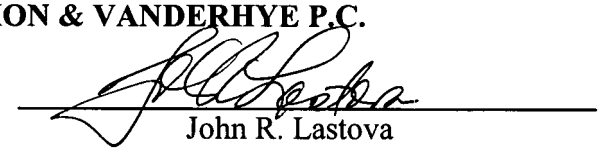
The SMI handler (equated by the Examiner to the monitor mode) also fails to manage the switching between secure and non-secure domains so as to ensure "that operation of the processor in said monitor mode is unaffected by the switching of the processor configuration data." As explained earlier, when processor configuration data is changed in the storage unit, it is immediately effective, which may compromise the ability of the monitor program to correctly switch of all of the required processor configuration data. That is the problem with Shipman's password. The password provides access and allows the switching to occur to a secure mode (see blocks 324 and 332 in Figure 14), but it does not ensure that no security compromise occurs during the switching operation. In contrast, this problem is overcome by the monitor program using monitor mode specific processor configuration data when the processor operates in the monitor mode, which ensures that the processor is not affected by the switching of the processor configuration data required to implement the transition from one domain to the other.

CONCLUSION

As demonstrated above, even if these two references could be combined as proposed they do not teach the combination of features recited in the independent claims. Moreover, the combination is difficult at best. Candelore's teachings relate to a dual mode processor. Shipman relates to an entirely different technical problem: the interaction between a system management interrupt (SMI) handler and a keyboard controller. For multiple reasons, the final rejection should be withdrawn and the application passed to allowance.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 

John R. Lastova
Reg. No. 33,149

901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100